

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of)	
)	
Agostinho DeArruda Villela)	Group Art Unit: 2431
)	
Serial No. 10/598,719)	Examiner: Wright, Bryan F
)	
Filed: September 8, 2006)	
)	
For: Access Control System For)	
Information Services Based)	
On Hardware And Software)	
Signature Of A Requesting)	
Device)	

APPEAL BRIEF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of)
)
Agostinho DeArruda Villela) Group Art Unit: 2431
)
Serial No. 10/598,719) Examiner: Wright, Bryan F
)
Filed: September 8, 2006)
)
For: Access Control System For)
Information Services Based)
On Hardware And Software)
Signature Of A Requesting)
Device)

APPEAL BRIEF

I. INTRODUCTION

This is an appeal from the decision mailed September 9, 2010 of the Patent Examiner, Group Art Unit 2431, finally rejecting claims 17-19, 22, 23, 26-28, 31 and 33-35 under 35 U.S.C. §103 as being obvious by Moshir in view of Bajikar and further in view of Nishibi, rejecting claims 20 and 21 under 35 U.S.C. §103 as being obvious by Moshir and Bajikar in view of Nishibi and in further view of Cui, rejecting claims 24 and 25 under 35 U.S.C. §103 as being obvious by Moshir and Bajikar in view of Nishibi and in further view of Abburri, and finally rejecting claims 29 and 30 under 35 U.S.C. §103 as being obvious by Moshir and Bajikar in view of Nishibi and in further view of Hyman.

II. REAL PARTY IN INTEREST

The Applicant is the real party in interest.

III. RELATED APPEALS AND INTERFERENCES

None.

IV. STATUS OF THE CLAIMS

Claims 17-35 stand rejected by the action mailed September 9, 2010. Claims 17-35 are pending. Applicant hereby appeals the rejection of claims 17-35.

V. STATUS OF AMENDMENTS

None.

VI. SUMMARY OF CLAIMED SUBJECT MATTER

Applicant's claim 17 claims a method for identifying devices and controlling access to a service (page 5, lines 1-7), comprising the steps of collecting data related to software and hardware configurations from a device through a software agent (page 5, lines 8-14), generating a digital signature (page 5, lines 15-20) for the device by hashing the software and hardware configuration data (page 8, lines 1-8), sending the digital signature of the device to an authentication server (page 5, lines 21-24), and determining whether the device has been excluded from accessing or enrolling in the service (page 9, lines 6-10).

Applicant's claim 31 claims a method for identifying devices and controlling access to a service (page 5, lines 1-7) comprising the steps of collecting data related to software and hardware configurations from the device through a software agent (page 5, lines 8-14), generating a digital signature (page 5, lines 15-20)

for the device by hashing the software and hardware configuration data (page 8, lines 1-8), sending the digital signature of the device to the authentication server (page 5, lines 21-24), verifying that the device is not on a list or in a group of devices not allowed to access the service (page 9, lines 6-10), or is not a device with a maximum number of enrollments set to zero (page 9, lines 6-10), and registering the device as authorized to access the service (page 7, lines 10-24).

Applicant's claim 35 claims a system for identifying devices and controlling access to a service (page 5, lines 1-7) comprising a software agent installed on a device (page 5, lines 8-14) adapted to collect data related to software and hardware configuration of the device (page 5, lines 8-14), a digital signature for the device generated by the software agent by hashing the software and hardware configuration data (page 8, lines 1-8), and an authentication server that determines whether the device can access the service based upon the digital signature of the device (page 5, lines 21-24), wherein the authentication server verifies that the device is not a list or in a group of devices not allowed to access the service (page 9, lines 6-10), or is not a device with a maximum number of enrollments set to zero (page 9, lines 6-10).

VII. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 17-19, 22, 23, 26-28, 31 and 33-35 stand rejected under 35 U.S.C. §103 as being obvious by Moshir in view of Bajikar and further in view of Nishibi. Claims 20 and 21 stand rejected under 35 U.S.C. §103 as being obvious by Moshir and Bajikar in view of Nishibi and in further view of Cui. Claims 24 and 25 stand rejected under 35 U.S.C. §103 as being obvious by Moshir and Bajikar in view of Nishibi and in further view of Abburi. Claims

29 and 30 stand rejected under 35 U.S.C. §103 as being obvious by Moshir and Bajikar in view of Nishibi and in further view of Hyman.

VIII. ARGUMENT

(A) Claim 17 rejected under Section 103

The examiner has rejected claim 17 under 35 U.S.C. §103 as being made obvious by Moshir in view of Bajikar and further in view of Nishibi.

Applicant's claim 17 is a method of identifying devices and controlling access to a service, i.e., a method of securing a computer. The Moshir reference has nothing whatsoever to do with identifying devices and controlling access to a service. The Moshir reference is a system for installing a software patch, which does so by first checking to make sure the computer's software and hardware is capable of accepting the patent. This crucial aspect of Applicant's invention is totally absent from all the cited references. As such, the examiner's position that "Moshir teaches a method of identifying devices and controlling access to a service" is erroneous.

Applicant's claim 17 also specifically describes the method as including the step of "collecting data related to software and hardware configurations from a device through a software agent". The examiner contends that the Moshir reference shows this feature. However, upon examination of the Moshir reference it is clear that this reference shows the gathering of stored software and hardware data (parameters), but does not show the gathering of software and hardware configurations, parameters are simply the basic identification of the software and hardware used (example, Windows 7) or "type" used in the system, while the configuration specifically identifies the specific hardware or software (example the serial number of such). Many computers may have the exact same

"parameters" but only one computer/system has a unique "configuration". The Moshir reference only shows that the system checks the software and hardware parameters that are necessary in order to install a software "patch". These software and hardware minimum parameters are stored in the inventory library 918. As such, these are simply stored values in a database. The comparison made in Moshir is not a "collecting" of data since the data is previously stored and therefore not "collected". Thus, the mere checking of a computer system to insure that it may accept a new software patch is a long cry from Applicant's claimed method which commences with the collecting of data relating to software and hardware configurations (in order to create a signature).

Applicant also submits that while Moshir eludes to the fact that software and hardware may be used insure a computer is capable of accepting a patch, the Moshir reference does not teach on how to collect data relating to software and hardware configuration. As such, the Moshir reference is non-enabling in this respect and therefore should not be utilized as a reference for establishing such.

Lastly, the Moshir reference does not describe the step of "generating a digital signature for the device by hashing the software and hardware configuration data". The examiner admits that this step is absent and therefore identifies the Bajikar reference. The Bajikar reference is for a method of providing a trusted time stamp. The time stamp may include a system parameter to aid in the verification process. Simply put, this is simply a trusted clock.

The examiner has not cited anything which would show a motivation, suggestion or otherwise for combining the software patch verification of Moshir with the time stamp operation of Bajikar. Without such motivation, it is improper for the examiner to combine these two references.

Furthermore, even if one were to combine these two references, the result would not be Applicant's method of identifying devices and controlling access to a service. The Bajikar reference again merely shows that a computer may access stored values in a database, see paragraph 0057 which recites

"For the computing system 100, for example, the hashing engine 182 may perform the hash using platform configuration parameters stored in the platform configuration register(s) 184".

Again, simply accessing stored data within a database does not show Applicant's method of collecting data related to software and hardware configurations from a device through a software agent and generating a digital signature from the device by hashing the software and hardware configuration data. It is respectfully submitted that the combination suggested by the examiner does not collect, generate, hash, to create a digital signature.

The examiner recognizes that even with the combination of the first two references a third reference must be brought in by the examiner to show the sending of a digital signature. For this reason the examiner has identified the Nishibi reference. The examiner specifically points to paragraph 227 to support his proposed combination. The entire paragraph 227 is recited as

Meanwhile, the key necessary for reciprocal authentication of the purchasing application program 115-2 and the content management program 111, and the key for managing the contents downloaded from the EMD servers 4-3 and 4-4, are transmitted as these keys are stored with a signature in a predetermined certificate.

Again, the Nishibi reference is relating the "storage" of data. Such data storage is not Applicant's claimed "sending the digital signature of the device to an authentication server". The Nishibi reference does not send a digital signature of the device. As the Nishibi reference does not complete the claimed step, it should not be utilized to render such obvious.

Lastly, Applicant's claim specifically states the step of "determining whether the device has been excluded from accessing or enrolling in the service". None of the references show the step of determining whether the device has been excluded. As none of the references show this crucial step, the combination of the cited references do not make obvious Applicant's method recited in Claim 17.

Applicant respectfully submits that the examiner has attempted to find a step from each of three references, but has not shown any motivation or suggestion of how or why one of ordinary skill in the art would combine these three references. Applicant further submits that such a motivation would be difficult, if not impossible, to show as each of the three references are directed to such different concepts: (1) Moshir a system for updating software patches, (2) Bajikar a method for providing a trusted time stamp, and (3) a device for program storage medium. As the Examiner has failed to make a prima facie case of obviousness under Section 103. The rejection contains no statement that supports a motivation to combine these three pieces of prior art to develop the Applicant's claimed invention, other than the conclusory assertion that one of ordinary skill in the art would have recognized the desirability and advantage of the combination. Conclusory statements of generalized advantages are inadequate to support a finding of motivation. See, e.g., *In re Beasley*, 2004 WL 2793170 (Fed. Cir. Dec. 7, 2004) (slip op. at 10). The examiner must present a "convincing line of reasoning" as to why the combination of

teachings is proper. MPEP 2142. There is no such line of reasoning in the rejection, and a prima facie case has not been made.

It is well settled that the obviousness of an invention cannot be established by combining the teaching of the prior art absent some teaching, suggestion or incentive supporting the combination, see *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *Ashland Oil, Inc. v. Delta Resins and Refractories, Inc.*, 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985) ; *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 221 USPQ 929 (Fed. Cir. 1984) *Pentec, Inc. v Graphic Controls Corp.*, 776 F.2d 309, 227 USPQ 766 (Fed. Cir. 1985). Moreover, the mere fact that the prior art could be modified in the manner suggested by the examiner does not make such a modification obvious unless the prior art fairly suggests the desirability of the modification, see *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) . Here, the references do not suggest any motivation for, or the desirability of, Applicant's unique method of utilizing hardware data to verify access and to exclude devices from accessing the service. As such, it is improper to utilize these references to establish obviousness.

It is acknowledged that the tendency to resort to "hindsight" based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art. MPEP 2142. This is "especially important in the case of less technologically complex inventions, where the very ease with which the invention can be understood may prompt one 'to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.'" *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999)

citing *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 313 (Fed. Cir. 1983) . With this in mind, a hindsight-based obviousness analysis must be supported by evidence which is "clear and particular". *In re Dembiczak*. It is insufficient to simply offer a broad range of sources or to make conclusory statements, as "[broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence'". *Id.* Applicant respectfully submits that the examiner has claimed the present invention to be obvious utilizing hindsight, speculation and conclusory statements which are not, in fact, supported by the cited references, to come up with a combination that would either destroy the clear intention of the reference or modify such in a manner that goes against the clear teachings of the reference. Furthermore, it is submitted that it is only through such hindsight that the Applicant's invention of an access control system and method can be gleaned from the cited references. Applicant respectfully contends that the invention is not obvious or a designer's choice, but instead is novel and therefore worthy of patent protection.

Applicant respectfully submits that the invention described in Claim 17 is novel and worthy of patent protection.

(B) Claim 31 under Section 103

The examiner has rejected claim 31 under 35 U.S.C. §103 as being made obvious by Moshir in view of Bajikar and further in view of Nishibi.

Applicant's claim 31 specifically describes the method as including the step of "collecting data related to software and hardware configurations from a device through a software agent". The Moshir reference has nothing whatsoever to do with identifying devices and controlling access to a service. The Moshir reference is a system for installing a software patch, which does so by first

checking to make sure the computer's software and hardware is capable of accepting the patent. This crucial aspect of Applicant's invention is totally absent from all the cited references. As such, the examiner's position that "Moshir teaches a method of identifying devices and controlling access to a service" is erroneous.

Applicant's claim 31 also specifically describes the method as including the step of "collecting data related to software and hardware configurations from a device through a software agent". The examiner contends that the Moshir reference shows this feature. However, upon examination of the Moshir reference it is clear that this reference shows the gathering of stored software and hardware data (parameters), but does not show the gathering of software and hardware configurations, parameters are simply the basic identification of the software and hardware used (example, Windows 7) or "type" used in the system, while the configuration specifically identifies the specific hardware or software (example the serial number of such). Many computers may have the exact same "parameters" but only one computer/system has a unique "configuration". The Moshir reference only shows that the system checks the software and hardware parameters that are necessary in order to install a software "patch". These software and hardware minimum parameters are stored in the inventory library 918. As such, these are simply stored values in a database. The comparison made in Moshir is not a "collecting" of data since the data is previously stored and therefore not "collected". Thus, the mere checking of a computer system to insure that it may accept a new software patch is a long cry from Applicant's claimed method which commences with the collecting of data relating to software and hardware configurations (in order to create a signature).

Applicant also submits that while Moshir eludes to the fact that software and hardware may be used insure a computer is capable

of accepting a patch, the Moshir reference does not teach on how to collect data relating to software and hardware configuration. As such, the Moshir reference is non-enabling in this respect and therefore should not be utilized as a reference for establishing such.

Lastly, the Moshir reference does not describe the step of "generating a digital signature for the device by hashing the software and hardware configuration data". The examiner admits that this step is absent and therefore identifies the Bajikar reference. The Bajikar reference is for a method of providing a trusted time stamp. The time stamp may include a system parameter to aid in the verification process. Simply put, this is simply a trusted clock.

The examiner has not cited anything which would show a motivation, suggestion or otherwise for combining the software patch verification of Moshir with the time stamp operation of Bajikar. Without such motivation, it is improper for the examiner to combine these two references.

Furthermore, even if one were to combine these two references, the result would not be Applicant's method of identifying devices and controlling access to a service. The Bajikar reference again merely shows that a computer may access stored values in a database, see paragraph 0057 which recites

"For the computing system 100, for example, the hashing engine 182 may perform the hash using platform configuration parameters stored in the platform configuration register(s) 184".

Again, simply accessing stored data within a database does not show Applicant's method of collecting data related to software and hardware configurations from a device through a software agent and

generating a digital signature fro the device by hashing the software and hardware configuration data. It is respectfully submitted that the combination suggested by the examiner does not collect, generate, hash, to create a digital signature.

The examiner recognizes that even with the combination of the first two references a third reference must be brought in by the examiner to show the sending of a digital signature. For this reason the examiner has identified the Nishibi reference. The examiner specifically points to paragraph 227 to support his proposed combination. The entire paragraph 227 is recited as

Meanwhile, the key necessary for reciprocal authentication of the purchasing application program 115-2 and the content management program 111, and the key for managing the contents downloaded from the EMD servers 4-3 and 4-4, are transmitted as these keys are stored with a signature in a predetermined certificate.

Again, the Nishibi reference is relating the "storage" of data. Such data storage is not Applicant's claimed "sending the digital signature of the device to an authentication server". The Nishibi reference does not send a digital signature of the device. As the Nishibi reference does not complete the claimed step, it should not be utilized to render such obvious.

Lastly, Applicant's claim specifically states the step of "verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero, and registering the device as authorized to access the service". None of the references show these steps of verifying and registering. As none of the references show this crucial steps, the combination of the

cited references do not make obvious Applicant's method recited in Claim 31.

Applicant respectfully submits that the examiner has attempted to find a step from each of three references, but has not shown any motivation or suggestion of how or why one of ordinary skill in the art would combine these three references. Applicant further submits that such a motivation would be difficult, if not impossible, to show as each of the three references are directed to such different concepts: (1) Moshir a system for updating software patches, (2) Bajikar a method for providing a trusted time stamp, and (3) a device for program storage medium. As the Examiner has failed to make a prima facie case of obviousness under Section 103. The rejection contains no statement that supports a motivation to combine these three pieces of prior art to develop the Applicant's claimed invention, other than the conclusory assertion that one of ordinary skill in the art would have recognized the desirability and advantage of the combination. Conclusory statements of generalized advantages are inadequate to support a finding of motivation. See, e.g., *In re Beasley*, 2004 WL 2793170 (Fed. Cir. Dec. 7, 2004) (slip op. at 10). The examiner must present a "convincing line of reasoning" as to why the combination of teachings is proper. MPEP 2142. There is no such line of reasoning in the rejection, and a prima facie case has not been made.

It is well settled that the obviousness of an invention cannot be established by combining the teaching of the prior art absent some teaching, suggestion or incentive supporting the combination, see *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *Ashland Oil, Inc. v. Delta Resins and Refractories, Inc.*, 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985) ; *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 221 USPQ 929 (Fed. Cir. 1984) *Pentec, Inc. v Graphic Controls Corp.*, 776 F.2d 309, 227 USPQ 766

(Fed. Cir. 1985). Moreover, the mere fact that the prior art could be modified in the manner suggested by the examiner does not make such a modification obvious unless the prior art fairly suggests the desirability of the modification, see *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) . Here, the references do not suggest any motivation for, or the desirability of, Applicant's unique method of utilizing hardware data to verify access and to exclude devices from accessing the service. As such, it is improper to utilize these references to establish obviousness.

It is acknowledged that the tendency to resort to "hindsight" based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art. MPEP 2142. This is "especially important in the case of less technologically complex inventions, where the very ease with which the invention can be understood may prompt one 'to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.'" *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999) citing *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 313 (Fed. Cir. 1983) . With this in mind, a hindsight-based obviousness analysis must be supported by evidence which is "clear and particular". *In re Dembiczak*. It is insufficient to simply offer a broad range of sources or to make conclusory statements, as "[broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence'". *Id.* Applicant respectfully submits that the examiner has claimed the present invention to be obvious utilizing hindsight, speculation and conclusory statements which are not, in fact, supported by the cited references, to come up with a

combination that would either destroy the clear intention of the reference or modify such in a manner that goes against the clear teachings of the reference. Furthermore, it is submitted that it is only through such hindsight that the Applicant's invention of an access control system and method can be gleamed from the cited references. Applicant respectfully contends that the invention is not obvious or a designer's choice, but instead is novel and therefore worthy of patent protection.

Applicant respectfully submits that the invention described in Claim 31 is novel and worthy of patent protection.

(C) Claim 35 under Section 103

The examiner has rejected claim 35 under 35 U.S.C. §103 as being made obvious by Moshir in view of Bajikar and further in view of Nishibi.

Applicant's claim 35 is a method of identifying devices and controlling access to a service, i.e., a method of securing a computer. The Moshir reference has nothing whatsoever to do with identifying devices and controlling access to a service. The Moshir reference is a system for installing a software patch, which does so by first checking to make sure the computer's software and hardware is capable of accepting the patent. This crucial aspect of Applicant's invention is totally absent from all the cited references. As such, the examiner's position that "Moshir teaches a method of identifying devices and controlling access to a service" is erroneous.

Applicant's claim 35 specifically describes the method as including the step of having "a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device" and "hashing the software and hardware configuration data". The examiner contends that the Moshir

reference shows this feature. However, upon examination of the Moshir reference it is clear that this reference shows the gathering of stored software and hardware data (parameters), but does not show the gathering of software and hardware configurations, parameters are simply the basic identification of the software and hardware used (example, Windows 7) or "type" used in the system, while the configuration specifically identifies the specific hardware or software (example the serial number of such). Many computers may have the exact same "parameters" but only one computer/system has a unique "configuration". The Moshir reference only shows that the system checks the software and hardware parameters that are necessary in order to install a software "patch". These software and hardware minimum parameters are stored in the inventory library 918. As such, these are simply stored values in a database. The comparison made in Moshir is not a "collecting" of data since the data is previously stored and therefore not "collected". Thus, the mere checking of a computer system to insure that it may accept a new software patch is a long cry from Applicant's claimed method which commences with the collecting of data relating to software and hardware configurations (in order to create a signature).

Applicant also submits that while Moshir eludes to the fact that software and hardware may be used insure a computer is capable of accepting a patch, the Moshir reference does not teach on how to collect data relating to software and hardware configuration. As such, the Moshir reference is non-enabling in this respect and therefore should not be utilized as a reference for establishing such.

Lastly, the Moshir reference does not describe the device as having "a digital signature for the device generated by the software agent by hashing the software and hardware configuration data". The examiner admits that this element is absent and

therefore identifies the Bajikar reference. The Bajikar reference is for a method of providing a trusted time stamp. The time stamp may include a system parameter to aid in the verification process. Simply put, this is simply a trusted clock.

The examiner has not cited anything which would show a motivation, suggestion or otherwise for combining the software patch verification of Moshir with the time stamp operation of Bajikar. Without such motivation, it is improper for the examiner to combine these two references.

Furthermore, even if one were to combine these two references, the result would not be Applicant's system for identifying devices and controlling access to a service. The Bajikar reference again merely shows that a computer may access stored values in a database, see paragraph 0057 which recites

"For the computing system 100, for example, the hashing engine 182 may perform the hash using platform configuration parameters stored in the platform configuration register(s) 184".

Again, simply accessing stored data within a database does not show Applicant's method of collecting data related to software and hardware configurations from a device through a software agent and generating a digital signature from the device by hashing the software and hardware configuration data. It is respectfully submitted that the combination suggested by the examiner does not collect, generate, hash, to create a digital signature.

The examiner recognizes that even with the combination of the first two references a third reference must be brought in by the examiner to show that the system includes an authentication server that determines whether the device can access the service based upon the digital signature of the device. For this reason the

examiner has identified the Nishibi reference. The examiner specifically points to paragraph 227 to support his proposed combination. The entire paragraph 227 is recited as

Meanwhile, the key necessary for reciprocal authentication of the purchasing application program 115-2 and the content management program 111, and the key for managing the contents downloaded from the EMD servers 4-3 and 4-4, are transmitted as these keys are stored with a signature in a predetermined certificate.

Again, the Nishibi reference is relating the "storage" of data. Such data storage is not Applicant's claimed "authentication server that determines whether the device can access the service". The Nishibi reference does not send a digital signature of the device. As the Nishibi reference does not complete the claimed step, it should not be utilized to render such obvious.

Lastly, Applicant's claim specifically states the system includes "the authentication server verifies that the device is not a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero". None of the references show these limitations. As none of the references show this crucial elements, the combination of the cited references do not make obvious Applicant's method recited in Claim 35.

Applicant respectfully submits that the examiner has attempted to find a step from each of three references, but has not shown any motivation or suggestion of how or why one of ordinary skill in the art would combine these three references. Applicant further submits that such a motivation would be difficult, if not impossible, to show as each of the three references are directed to

such different concepts: (1) Moshir a system for updating software patches, (2) Bajikar a method for providing a trusted time stamp, and (3) a device for program storage medium. As the Examiner has failed to make a prima facie case of obviousness under Section 103. The rejection contains no statement that supports a motivation to combine these three pieces of prior art to develop the Applicant's claimed invention, other than the conclusory assertion that one of ordinary skill in the art would have recognized the desirability and advantage of the combination. Conclusory statements of generalized advantages are inadequate to support a finding of motivation. See, e.g., *In re Beasley*, 2004 WL 2793170 (Fed. Cir. Dec. 7, 2004) (slip op. at 10). The examiner must present a "convincing line of reasoning" as to why the combination of teachings is proper. MPEP 2142. There is no such line of reasoning in the rejection, and a prima facie case has not been made.

It is well settled that the obviousness of an invention cannot be established by combining the teaching of the prior art absent some teaching, suggestion or incentive supporting the combination, see *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *Ashland Oil, Inc. v. Delta Resins and Refractories, Inc.*, 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985) ; *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 221 USPQ 929 (Fed. Cir. 1984) *Pentec, Inc. v Graphic Controls Corp.*, 776 F.2d 309, 227 USPQ 766 (Fed. Cir. 1985). Moreover, the mere fact that the prior art could be modified in the manner suggested by the examiner does not make such a modification obvious unless the prior art fairly suggests the desirability of the modification, see *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) . Here, the references do not suggest any motivation for, or the desirability of, Applicant's unique method of utilizing hardware data to verify access and to exclude devices from accessing the service. As such,

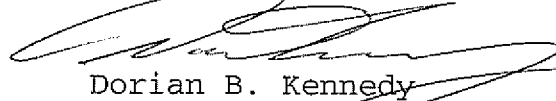
it is improper to utilize these references to establish obviousness.

It is acknowledged that the tendency to resort to "hindsight" based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art. MPEP 2142. This is "especially important in the case of less technologically complex inventions, where the very ease with which the invention can be understood may prompt one 'to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.'" *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999) citing *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 313 (Fed. Cir. 1983) . With this in mind, a hindsight-based obviousness analysis must be supported by evidence which is "clear and particular". *In re Dembiczak*. It is insufficient to simply offer a broad range of sources or to make conclusory statements, as "[broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence'". *Id.* Applicant respectfully submits that the examiner has claimed the present invention to be obvious utilizing hindsight, speculation and conclusory statements which are not, in fact, supported by the cited references, to come up with a combination that would either destroy the clear intention of the reference or modify such in a manner that goes against the clear teachings of the reference. Furthermore, it is submitted that it is only through such hindsight that the Applicant's invention of an access control system and method can be gleaned from the cited references. Applicant respectfully contends that the invention is not obvious or a designer's choice, but instead is novel and therefore worthy of patent protection.

Applicant respectfully submits that the invention described in Claim 35 is novel and worthy of patent protection.

The requisite fee due upon filing of this brief was previously attached. Any additional fee is to be charged to Baker Donelson Bearman Caldwell & Berkowitz, PC, Deposit Account No. 11-0553.

Respectfully submitted,



Dorian B. Kennedy
Registration No. 38,840

BAKER DONELSON BEARMAN CALDWELL & BERKOWITZ
Suite 1600
3414 Peachtree Road NE
Atlanta, Georgia 30328
(678) 406-8705

Docket No.: 2171323-000002

CLAIMS APPENDIX

Claims 1-16 (canceled).

Claim 17. A method for identifying devices and controlling access to a service, comprising the steps of:

collecting data related to software and hardware configurations from a device through a software agent;

generating a digital signature for the device by hashing the software and hardware configuration data;

sending the digital signature of the device to an authentication server; and

determining whether the device has been excluded from accessing or enrolling in the service.

Claim 18. The method of claim 17, wherein the digital signature sent to the authentication server is encrypted.

Claim 19. The method of claim 17, wherein the software agent is installed on the device as part of the process of using the device to access a service.

Claim 20. The method of claim 17, wherein the hashes used to generate the digital signature are changed with every attempt to access a service, and the hashes cannot be reversed.

Claim 21. The method of claim 17, wherein the digital signature is one of several stages of a framework of authorization and authentication processes governing access to the service by the device.

Claim 22. The method of claim 17, wherein the authentication server compares the digital signature sent with one or more previously-stored digital signatures.

Claim 23. The method of claim 17, wherein the authentication server determines whether the device has been excluded from accessing or enrolling in the service by determining whether the device is on a list or in a group of devices not allowed to access the service, or is included within a group of devices allowed to access the service.

Claim 24. The method of claim 17, wherein the authentication server allows a maximum number of enrollments for a particular device.

Claim 25. The method of claim 24, wherein the maximum number of enrollments is zero.

Claim 26. The method of claim 22, wherein the authentication server allows minor modifications to the software or hardware configurations of a previously-enrolled device so as to preserve access or denial of access for the device.

Claim 27. The method of claim 26, wherein the previously-stored digital signature of the device is updated to reflect the modifications.

Claim 28. The method of claim 17, wherein the authentication server logs all accesses or attempted accesses by a device to the service.

Claim 29. The method of claim 17, wherein multiple devices can be registered for a single user with the authentication server to create a registration hierarchy.

Claim 30. The method of claim 29, wherein a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered.

Claim 31. A method for identifying devices and controlling access to a service, comprising the steps of:

- collecting data related to software and hardware configurations from the device through a software agent;

- generating a digital signature for the device by hashing the software and hardware configuration data;

- sending the digital signature of the device to the authentication server;

- verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero;

- and registering the device as authorized to access the service.

Claim 32. The method of claim 31, further comprising the step of verifying the identity of the device each time it subsequently attempts to access the service.

Claim 33. The method of claim 32, wherein the step of verifying the identity of the device comprises the steps of:

- collecting data related to current software and hardware configurations from the device through a software agent;

- generating a digital signature for the device by hashing the

software and hardware configuration data;

sending the digital signature of the device to the authentication server; and

comparing the digital signature sent with one or more previously-stored digital signatures for the device.

Claim 34. The method of claim 32, wherein the step of verifying the identity of the device comprises the steps of:

collecting data related to current software and hardware configurations from the device through a software agent;

generating a digital signature for the device by hashing the software and hardware configuration data;

sending the digital signature of the device to the authentication server; and

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero.

Claim 35. A system for identifying devices and controlling access to a service, comprising:

a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device;

a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data; and

an authentication server that determines whether the device can access the service based upon the digital signature of the device;

wherein the authentication server verifies that the device is not a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None